

(19) World Intellectual Property Organization
International Bureau



(43) International Publication Date
3 January 2002 (03.01.2002)

PCT

(10) International Publication Number
WO 02/01331 A2

(51) International Patent Classification⁷: **G06F 1/00**

(21) International Application Number: PCT/US01/20684

(22) International Filing Date: 27 June 2001 (27.06.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/214,464 27 June 2000 (27.06.2000) US

(71) Applicant and

(72) Inventor: **CLARK, James, R.** [US/US]; 1470 W. 116 Avenue #22, Westminster, CO 80234 (US).

(74) Agent: **PEDERSEN, Ken, J.**; Pedersen & Company, PLLC, 1410 North 28th Street, Boise, ID 83703 (US).

(81) Designated States (*national*): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU,

CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

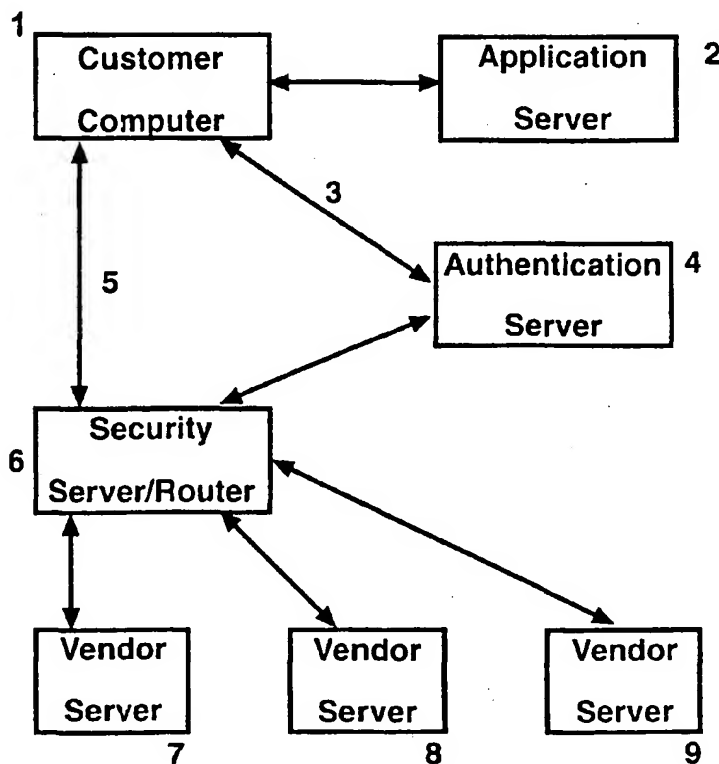
(84) Designated States (*regional*): ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:

— without international search report and to be republished upon receipt of that report

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: **PERSONAL COMPUTER SECURED INTERNET DEVICE**



(57) Abstract: The present invention relates to digitally encoded copyrighted or otherwise proprietary data of any kind. More specifically, the present invention relates to a secured system for authentication and registration of any Internet device, said authentication and registration being required by the novel system before said Internet devices are afforded access to said data. Said authentication is accomplished by first requiring a user to access an application server. The application server allows the user to download a novel software application which is used to determine a unique Internet device access number. Once a unique Internet device access number is determined, the user may access the novel system through an authentication server. The authentication server authenticates and registers the unique Internet device access number prior to affording access to the system's security server/router. The user may then access vendor servers containing copyrighted or otherwise proprietary data. In this way, the novel system transforms any Internet device into a secure Internet device (SID).

WO 02/01331 A2

PERSONAL COMPUTER SECURED INTERNET DEVICE

DESCRIPTION

BACKGROUND OF THE INVENTION

5 Field of the Invention.

Embodiments of the present invention relate to digitally encoded copyrighted or otherwise proprietary data of any kind. More specifically, the present invention relates to a secured system for authentication and registration of any Internet device, said authentication and registration being required by the novel system before said Internet devices are afforded access to said data. Said authentication is accomplished by first requiring a user to access an application server. The application server allows the user to download a novel software application which is used to determine a unique Internet device access number. Once a unique Internet device access number is determined, the user may access the novel system through an authentication server. The authentication server authenticates and registers the unique Internet device access number prior to affording access to the system's security server/router. In this way, the novel system transforms any Internet device into a Secure Internet Device (SID).

As an introduction to the problems solved by the present invention, consider the development of present-day MP3 type players. MP3 technology allows users to download audio and music content over the Internet for play on MP3 compatible playing devices, including those that are portable and those internal to a personal computer. From the point of view of the audio and music content recording industry, a major drawback to the presently available MP3 devices and technologies is that they afford virtually no protection against copyright infringements by either Internet MP3 sourcing parties, nor by MP3 end users. The present invention remedies this functional deficiency through a novel and innovative process for controlling access to media content. This system can protect any type of digitally encoded data that can be transmitted via the Internet by providing a system which restricts access to only those Internet devices which have been first authorized and registered utilizing a unique hardware identifier associated with each such device.

SUMMARY OF THE INVENTION

The present invention relates to a system which is capable of converting any Internet device into a SID. More specifically, the present invention utilizes a novel software application which is used to determine a unique identification number for any Internet device. For example, any personal computer (PC) capable of accessing the Internet may access an application server to download the software application which determines a unique Internet device access number. The PC may then be authenticated through an authentication server. The authentication server identifies and registers the unique access number of the PC. Only PCs which have been authenticated and registered are afforded access to vendor servers. Access is afforded in a manner consistent with pre-existing contracts established through a customer service center. All access to vendor servers is tracked via the unique access number, such that said access may be billed according to said predetermined contract. In this manner, any PC may become a SID.

Once the Internet device is authenticated, it may access a security server/router. For example, an authenticated PC (i.e. "PCSID") may access the security server/router which then routes requests to various vendor servers comprising a copyrighted data library across the Internet. This data could be any copyrighted digital data including digital Music or Video. This data would only be available to customers who have an Internet device which has been authenticated through the authentication server. In this way, the security server/router may identify the unique customer and cross reference them to a customer data base for billing.

For example, with a PC, these customers access the application server, download the novel software application which identifies a unique access number for the PC, and then register their account via an authentication server or a free access (800) telephone number utilizing a service center located at said authentication server or a free access (800) telephone number. The service center collects customer information including address, phone number, and payment information, and the unique access number of the PCSID is authenticated and registered. The service center then transfers the information to the security server/router. The security server/router will only afford access to PCs which have been so authenticated and registered. Then the customer could connect through the security server/router to the data service providers via various vendor servers. With the novel system, secure access and secure

downloading of audio and music content, and the like, would be achieved, such that each user can pick their own listening collections, and the provider can maintain copyright protection security. The control given by this restricted accessibility provides a cost-effective solution to the legal problems that have recently arisen from unauthorized distribution of copyright
5 protected audio and music content over the Internet.

This invention incorporates a unique serial number for each Internet device, creating a SID. This could be a MAC code on a network card, a serial number in an EPROM, or a unique identification number on a CPU or other IC of any type. For example, the unique identification embedded in each Pentium III® chip could serve as a PC specific identifier used
10 to authenticate and register the specific PC requesting access. As long as this identifier was authenticated and registered, the novel system will allow the user access. This number is registered with the system web site through which access to the copyrighted content is given, along with the customer credit card or other means of billing fees (i.e. direct electronic transfer from checking accounts, etc.).

Once the user is registered, the then-operational Internet device can be used to
15 access the provider servers, which give access to copyrighted content libraries, on a per title basis. For marketing promotions, pre-selected portions of titles could be made available for free review (by prior arrangements with copyrighted content providers). Once titles are selected for downloading, charges are made to the customer's account. Each account is billed
20 to the pre-arranged credit card on a monthly basis.

It is an object of the present invention to overcome deficiencies in current technology which make it impossible to adequately protect copyrighted or otherwise proprietary data made available over the Internet. A further object of the present invention is to provide a system which allows any Internet device to access data over the Internet while
25 simultaneously protecting the copyright interests of the data providers. For example, Internet devices such as personal computers may access the copyrighted content libraries through the novel system. Said access is first authenticated through a unique hardware identifier on the PC, such as, for example, the unique ID built into each Pentium III® chip. Any data provided to an Internet device, such as a PC, which may digitally reproduce said data, shall be provided in a
30 format which includes a unique identifier, such as an electronic watermark. As a result, any digital reproduction of said data may be readily identified and attributed to the uniquely

authenticated Internet device which originally accessed said data. Therefore, the novel system facilitates secure access to copyrighted data from any Internet device via any means of access (modem, ethernet, RF, cellular, etc.).

5 These and other embodiments, aspects, advantages and features of the present invention will be set forth in part in the description, and in part will come to those skilled in the art by reference to the following description of the invention and referenced drawings, or by practice of the invention.

BRIEF DESCRIPTION OF THE DRAWINGS

10

Figure 1 is a schematic diagram of the inter-networked system components according to one embodiment of the invention employing a modem-connected PC.

Figure 2 is a flowchart of a sample PC Secured Internet Device Internet Distribution System according to one embodiment of the invention.

15

DETAILED DESCRIPTION OF THE INVENTION

The novel system transforms any Internet device into a Secured Internet Device (SID) by using a novel software application to create a unique access number used to identify any such device. As such, an Internet distribution system is created which provides a means of
20 affording facile access to copyrighted or otherwise proprietary data over the Internet while simultaneously protecting the copyright interests of the data providers. The system requires that a unique identifier be authenticated and registered before any Internet device is allowed to access said system's data service providers through various vendor servers. Furthermore, the novel system incorporates the unique access number into an electronic watermark which is
25 embedded within any data downloaded from said vendor servers so that any unauthorized re-distribution of said data would be easily traced to the original source of said re-distribution.

Referring to the figures, Figure 1 is a schematic diagram of one embodiment of the present invention. Figure 1 shows the inter-networked copy-protected Internet distribution system components employing a modem-connected PC 1. Representative Vendor Servers 7, 8,
30 and 9, are connected to a Security Router/Server 6.

In order to access the novel system, the PC 1 must first access an Application Server 2. The Application Server 2 allows the PC 1 to download a novel software application which determines a unique access number for the PC 1. Said unique access number is called a Secured Internet Device access number. Once the unique access number is determined, the PC 1 is enabled as a Secured Internet Device, or "PCSID".

The PCSID 1 may then contact the Authentication Server 4 via virtual private network link 3. A customer service center at the Authentication Server 4 obtains customer information including address, phone number, and payment information. The Authentication Server 4 also authenticates and registers the PCSID 1 access number. It is also envisioned that, as an alternative to the Authentication Server 4, the PCSID 1 may also connect to the customer service center via a free access (800) telephone number. Said service center would collect customer information and authenticate PCSID 1 access numbers in the manner described above.

The Authentication Server 4 then transfers the information to the Security Server/Router 6. The Security Server/Router 6 stores customer information provided by the Authentication Server 4 so that the PCSID 1 may subsequently access the Security Server/Router 6 via virtual private network link 5 without first accessing the Authentication Server 4. Once authenticated, the PCSID may access the vendor servers 7, 8, and 9 through the Security Server/Router 6. The Security Server/Router 6 tracks customer use including downloading of music or other data. This provides the detailed reports necessary for billing customers and providing royalty payments due to authors, composers and other such owners of copyrighted or otherwise protected data.

The novel system provides security and control for data from Vendor Servers 7, 8, and 9 to customer's PCSID 1 or any other Internet device made secure by the novel system. Because the customer's PCSID 1 may allow digital storage and duplication of data so provided, it is also envisioned that an extra layer of protection is provided via electronic watermark technology. This is accomplished by embedding the unique Secured Internet Device access number within an electronic watermark contained in all data accessed through the novel system. Using the Secured Internet Device access number embedded in the watermark, tracking of any unauthorized re-distribution of the digital data would be straightforward as it would be easy to verify the source of the re-distribution.

Once the PCSID 1 is validated as a registered device, then requests for media sampling and/or download can be serviced directly via the Security Server/Router 6 via virtual private network link 5 without first accessing the Authentication Server 4. If download requests are made on behalf of a PCSID 1 via the Security Server/Router 6, then encrypted download information is sent from Vendor Servers 7, 8, and 9 to customer's PCSID 1 through Security Server/Router 6 and virtual private network link 5. Included in said encrypted download information is an electronic watermark in which is embedded the SID access number which may be used to uniquely identify the source of any subsequently re-distributed copies of said information.

Figure 2 depicts a flowchart of the SID distribution system registration process utilizing a PC as a sample Internet device. First, the customer accesses the Application Server 10. The customer then downloads the novel software application onto the customer's PC 11. The novel software application then determines an access number which is unique to the particular PC 12. The PC, now enabled as a PCSID, then accesses the Authentication Server 13. If the customer is accessing the novel system for the first time, the Authentication Server authenticates and registers the unique access number of the PCSID 15. A customer service center located at the Authentication Server records customer billing information 16. The authenticated PCSID is then allowed access Security Server/Router 17. The Security Server/Router affords the customer access to Vendor Servers from which the customer may sample or purchase content 18. Any data downloaded by the customer is tracked via the unique access number determined by the novel software application. Once a customer's PC has been authenticated and registered 15, and all customer billing information has been obtained 16, subsequent access to the system is granted on the basis of the authenticated unique access number 14, thus eliminating the need for steps 15 and 16, above. It is also envisioned that Once a customer's PC has been authenticated and registered 15, and all customer billing information has been obtained 16, all customer data may be stored on the Security Server/Router thereby allowing subsequent customer access to the Security Server/Router without first requiring access to the Authentication Server. Once authenticated and registered, the PC can be used freely within the conditions established by the service provider for sampling and usage of titles, groups of titles, other content, or other promotional schemes.

The benefits that will be attained through the use of the present invention are multiple. For the end customer, this system provides legal access control to copyrighted music, for a low cost and also it gives great flexibility in content selection. For the recording industry, this invention provides a direct low cost Internet distribution capability that protects
5 copyrighted music and other proprietary data, and derives a steady income stream. It also provides the capability to introduce and promote new artists with small followings with minimal cost.

For the various service providing companies, multiple income streams can be realized through patent licensing fees, fees per title, and advertising fees on the
10 world-wide-web site. The service provider will also gain an ability to promote its own and new artists in a cost-effective manner.

Although this invention has been described above with reference to particular means, materials and embodiments, it is to be understood that the invention is not limited to these disclosed particulars, but extends instead to all equivalents within the scope of the
15 following claims.

CLAIMS

I claim:

- 1 1. A secured system for access to data over the Internet, the secured system
2 comprising:
3 a customer's Internet device having a unique access number;
4 an application server accessible by said customer's Internet device;
5 a software application resident in said application server, said software application
6 being downloadable by said customer's Internet device to determine said unique access number
7 of said customer's Internet device; and
8 an authentication server also accessible by said customer's Internet device, said
9 authentication server being adapted to provide access of said customer's Internet device to
10 Internet data when said unique access number of said customer's Internet device has been
11 determined, authenticated and registered by said authentication server.

- 1 2. The secured system of Claim 1 wherein said authentication server provides access
2 of said customer's Internet device to a security server/router which in turn provides access to a
3 vendor server containing copyrighted or otherwise proprietary data.

- 1 3. A method for providing secure access to data over the Internet, the method
2 comprising:
3 requiring a user of an Internet device with a unique access number to access an
4 application server;
5 downloading a software application from said application server to said Internet
6 device;
7 determining said unique access number of said Internet device with the downloaded
8 software application; and
9 providing access to the Internet data through an authentication server which
10 authenticates and registers said Internet device unique access number.

1 4. The method of Claim 3 wherein access is provided through the authentication server
2 to a security server/router which in turn provides access to a vendor server containing
3 copyrighted or otherwise proprietary data.

1 5. The method of Claim 3 wherein the accessed Internet data is marked to identify it to
2 said unique access number.

1/2

